DEPARTMENT OF TECHNOLOGY & INFORMATION

DELIVERING TECHNOLOGY THAT INNOVATES

DO'S AND DON'TS FOR ONLINE PURCHASES

The holiday shopping season is underway and buying gifts online is more popular than ever. In this issue you'll find tips and information to protect yourself from identity theft and fraud. As you're making your holiday "to do" lists, add a cyber safety review at the top. Being an educated and aware online shopper will help to keep the holiday season merry and bright.

DO

Secure electronic devices. Use and update antivirus/ spam protection and update/patch operating systems, software, and apps.

Use passphrases. The longer the better…it's worth the extra key strokes! Use a mixture of numbers, special characters and upper and lower case letters and create unique passphrases for each site.

Know your online shopping merchants. Use merchants you know and trust. Confirm the seller's physical address and get a phone number in case you need to call them.

Pay all online transactions with one credit card. By using one credit card with a low credit limit you limit the potential for financial fraud to affect all of your accounts. Always check your statements regularly and carefully.

Look for website security. The "s" in "https" stands for "secure" and indicates that communication with the webpage is encrypted, This ensures information is transmitted safely to the merchant. Look for the padlock symbol in the web site address area.

Block pop-ups. They could be social engineering attempts designed to get you to open malware or a malicious link.

Use common sense to avoid scams. Don't give out your personal or financial information via email or text.

Review site privacy policies. Know what information merchants collect, how they store and use the information and if the information will be shared with others.

DON'T

Don't auto-save personal information. Ask yourself if the convenience is really worth the risk and remember that you will spend a great deal of time trying to repair the loss of your stolen personal information.

Don't use public computers or public wireless Internet. Increased risk includes viruses, malware, information and/ or identity theft and financial fraud.

Don't opt out on multi-factor authentication. It's been around for years—every social media platform makes it available to customers, yet many aren't using it. Research sites you use and choose multi-factor authentication.

IF YOU RUN INTO PROBLEMS

If you encounter problems with an online shopping site, contact the seller or the site operator directly to resolve any issues.

You may also report problems and request help from the Delaware Attorney General's Office, Better Business Bureau or the Federal Trade Commission.

TIPS FOR EMAIL AND TEXT MESSAGING

Be wary of emails and texts that appear to be from major retailers (like Walmart, Target or Amazon) that offer gift cards, special discounts or "alert" you to a problem with a recent purchase. These contacts may not be legitimate. Don't act on these messages; delete them and contact the retailer directly.

eSecurity Newsletters

Questions, comments or topic suggestions? Email us at eSecurity@state.de.us.

Visit digiknow.delaware.gov for previous issues.

DigiKnow CYBER SECURITY DEPENDS ON YOU